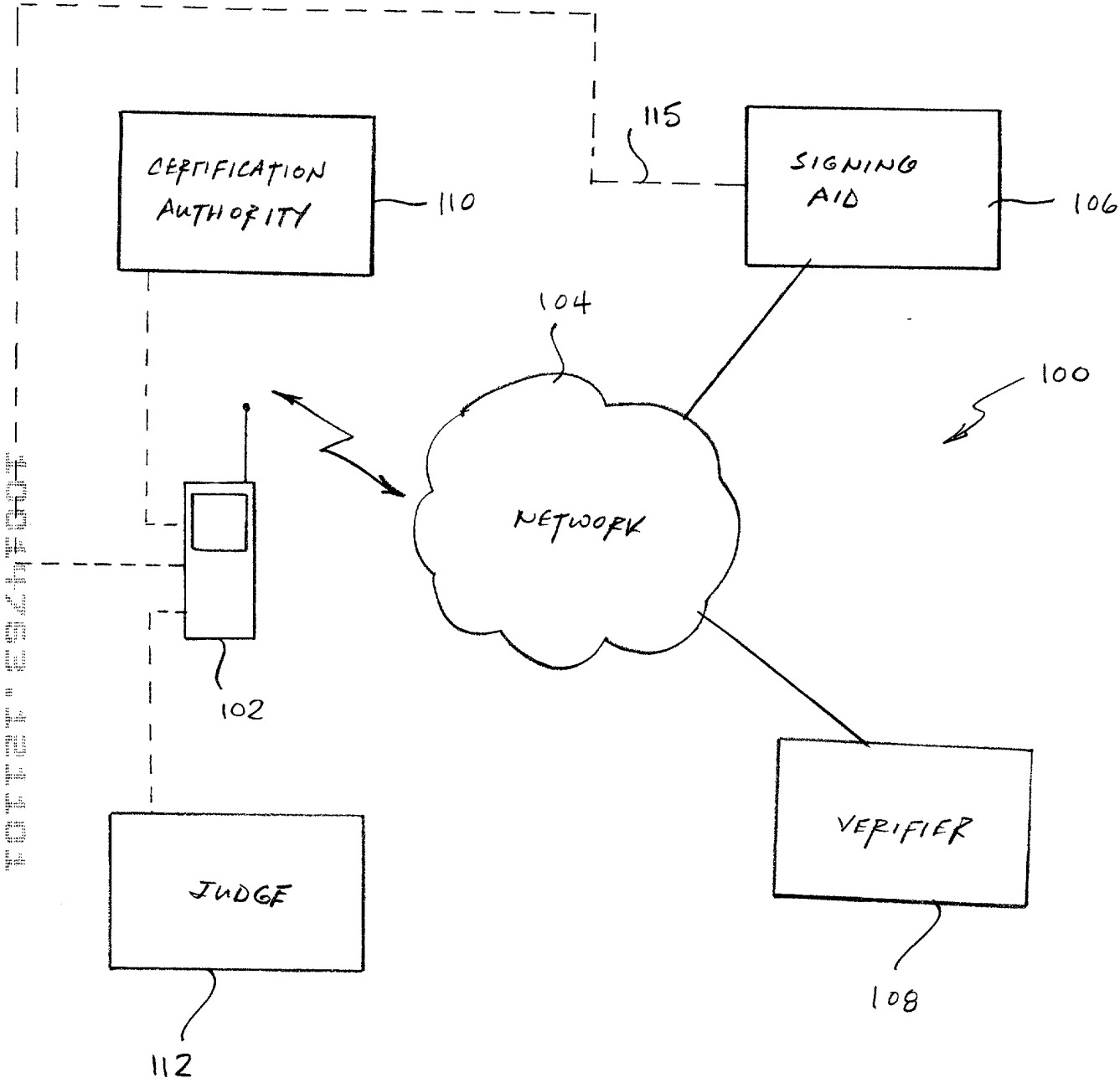
CERTIFICATION AUTHORITY
110
115
SIGNING AID
106
104
100
NETWORK
102
JUDGE
112
VERIFIER
108

FIG. 1

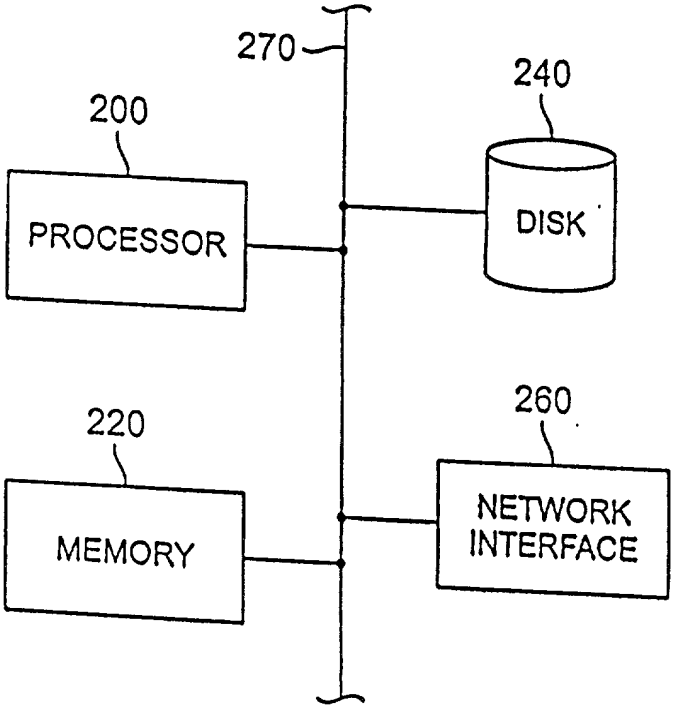
270
240
200
PROCESSOR
DISK
220
260
MEMORY
NETWORK
INTERFACE

FIG. 2

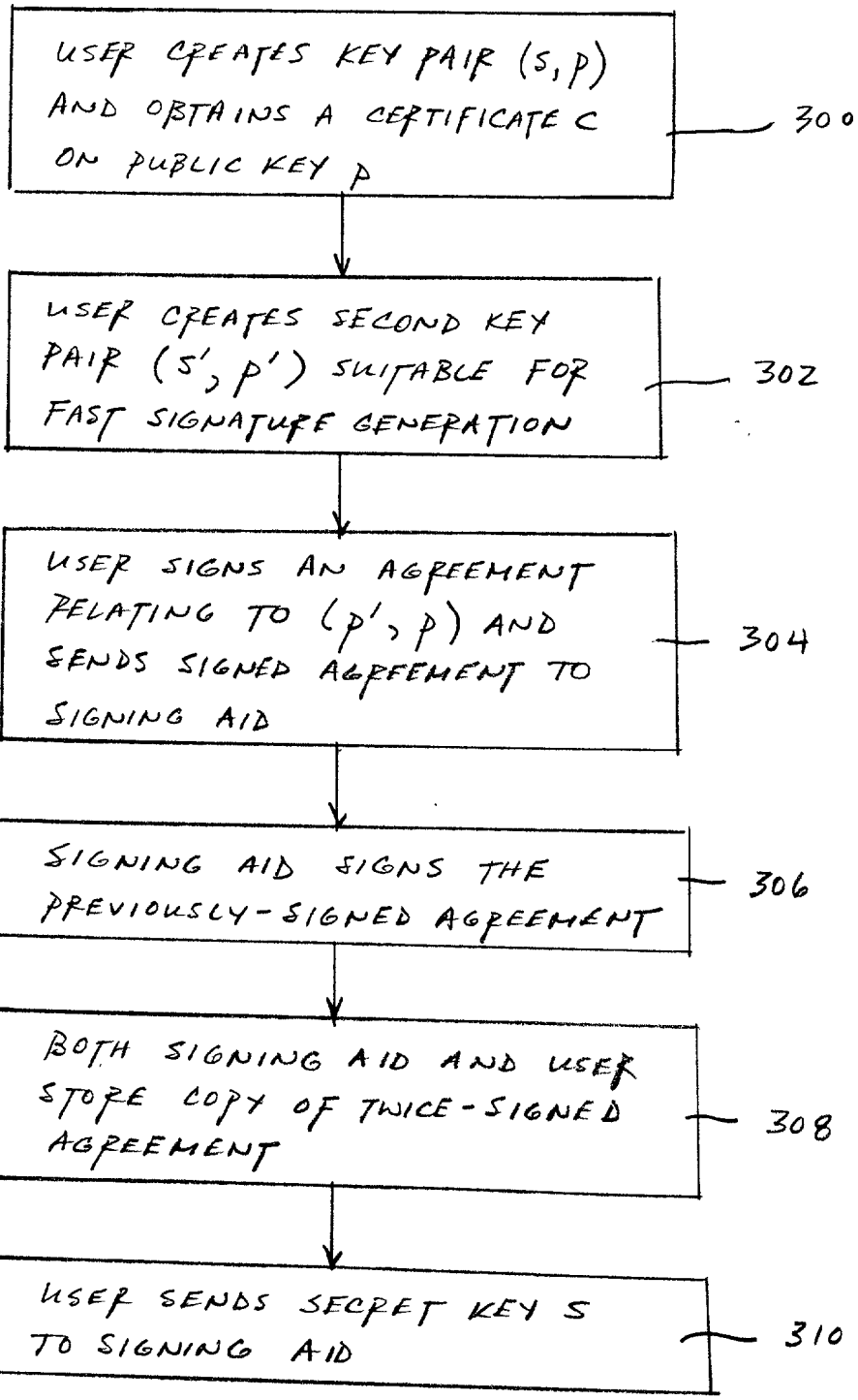
USER CREATES KEY PAIR (S, P) AND OBTAINS A CERTIFICATE C ON PUBLIC KEY P
300
USER CREATES SECOND KEY PAIR (S', P') SUITABLE FOR FAST SIGNATURE GENERATION
302
USER SIGNS AN AGREEMENT RELATING TO (P', P) AND SENDS SIGNED AGREEMENT TO SIGNING AID
304
SIGNING AID SIGNS THE PREVIOUSLY-SIGNED AGREEMENT
306
BOTH SIGNING AID AND USER STORE COPY OF TWICE-SIGNED AGREEMENT
308
USER SENDS SECRET KEY S TO SIGNING AID
310

FIG. 3

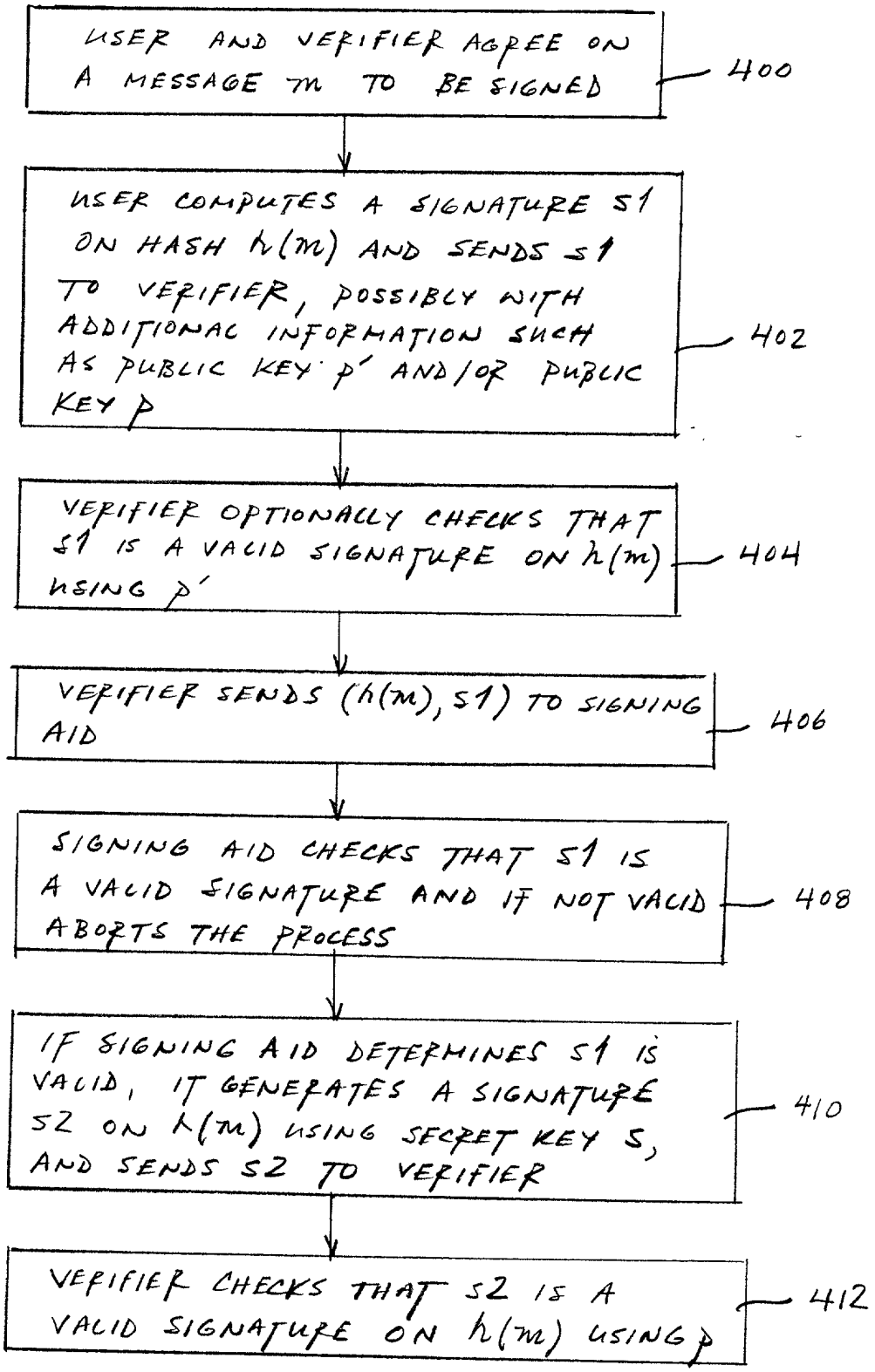
USER AND VERIFIER AGREE ON A MESSAGE m TO BE SIGNED
400
USER COMPUTES A SIGNATURE S1 ON HASH h(m) AND SENDS S1 TO VERIFIER, POSSIBLY WITH ADDITIONAL INFORMATION SUCH AS PUBLIC KEY p' AND/OR PUBLIC KEY p
402
VERIFIER OPTIONALLY CHECKS THAT S1 IS A VALID SIGNATURE ON h(m) USING p'
404
VERIFIER SENDS (h(m), S1) TO SIGNING AID
406
SIGNING AID CHECKS THAT S1 IS A VALID SIGNATURE AND IF NOT VALID ABORTS THE PROCESS
408
IF SIGNING AID DETERMINES S1 IS VALID, IT GENERATES A SIGNATURE S2 ON h(m) USING SECRET KEY S, AND SENDS S2 TO VERIFIER
410
VERIFIER CHECKS THAT S2 IS A VALID SIGNATURE ON h(m) USING p
412

FIG. 4